ソリューション概要

proofpoint.

PROOFPOINT CLOSED-LOOP EMAIL ANALYSIS AND RESPONSE

ワンクリックでフィッシングのリスクを低減

製品

- PhishAlarm
- PhishAlarm Analyzer
- Threat Response Auto-Pull (TRAP)

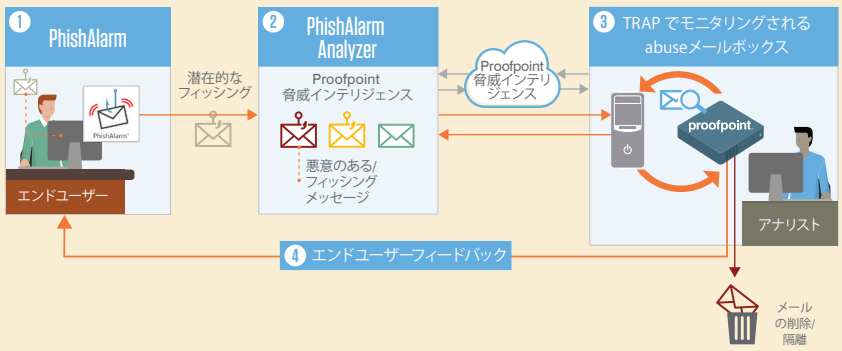
主な利点

- エンドユーザーは不審なメッセージをワンクリックで報告でき、メッセージは自動的に分析及び修復される
- 自動化による時間の節約：送信者のメールボックスから悪意のあるメッセージを排除し、転送されたメッセージを追跡して削除・隔離
- 独自の Proofpoint 脅威インテリジェンスを使用し、修復プロセスを効率化
- 実行したアクションの詳細及び履歴 (監査に利用可能) を提供

セキュリティ意識が高く、適切に訓練された従業員は安全なメールとフィッシングメールを区別することができます。フィッシングが疑われるメールに気づいた場合、通常はフィッシングメールをセキュリティチームまたはabuseメールボックスへ転送するなどといった対応を取ります。しかし、それに対応するチームは、報告された脅威を迅速に優先順位付けし対応するための十分な手段を持っていません。そのためリスクにさらされる時間が長くなり、組織への全体リスクも高まります。フィッシングを捕捉できないと、社内セキュリティチームは潜在的なキャンペーンを識別するチャンスや、より大規模なフィッシングの猛攻撃にあう前に防御策を改善するといったチャンスを逃してしまうことになります。Proofpoint Closed-Loop Email Analysis and Response (CLEAR) は、実際の攻撃によって業務の生産性が低下することを防ぎ、企業への財務的な影響を低減させます。

CLEAR はワンクリックでアクティブな攻撃を可視化し、また潜在的なフィッシング攻撃への自動化されたインテリジェントな分析レイヤーと修復機能を提供します。CLEARは、PhishAlarm（不審メール報告ボタン）、PhishAlarm Analyzer（Proofpoint 脅威インテリジェンスを用いた脅威の分類及び優先順位付け）、Threat Response Auto-Pull（TRAP：メール管理及び自動修復）を含む完全なソリューションです。

CLEARワークフロー



1つのボタンで機能強化

PhishAlarmボタンを導入することで、セキュリティチームは従業員が報告するフィッシングメールに対し、より優れたビジビリティを得られるようになります。

PhishAlarm のユーザーは不審なメールを受け取ると、これまで通り「フィッシングを報告」ボタンをクリックします。CLEARが導入されている場合は、PhishAlarm がこのメールを PhishAlarm Analyzer に送信します。

PhishAlarm Analyzerは、報告されたメールに含まれる脅威をサンドボックス環境で検査し、Proofpoint脅威インテリジェンスを活用してスコアを付け、分類します。その結果出された最新のスコアは、優先順位付けとTRAPでの処理に活用されます。TRAP はセキュリティ オートメーションとオーケストレーションを使って脅威コンテキストを追加し、企業全体で不正メールとそれに関連するインスタンスを自動的に特定します。

オートメーションでの保護

TRAP はabuseメールボックスに新しいメールが届いていないかを継続的にチェックし、届いていた場合はメッセージの削除や隔離を行います。

TRAPは複数のインテリジェンスとレピュテーションシステムを使用してこれらを数秒で分析し、実際に悪意のあるコンテンツが含まれていないかどうかを検証します。

また、TRAP はIP アドレスの地理的ロケーションを特定することができます。そして、不審なメールを最近の攻撃キャンペーンに自動的に紐付けることで、追加作業なしに潜在的脅威を可視化することができるようになります。セキュリティチームはこの知見をもって、ユーザーとデータを保護する行動を迅速に起こすことができるようになります。

TRAP では業界最高のレピュテーションフィードとインテリジェンス フィードが事前設定されています。またメールのビジネス ロジックにもあらかじめ紐付けられています。これによってTRAP は、クレデンシャルフィッシングのテンプレート、マルウェアのリンク、そして添付が含まれるメールを速やかに発見して対処できるようになります。

初期設定のままで使用できるその他の機能には、インシデント対応とレポーティングがあります。セキュリティチームは初期設定以外のコーディングやインテグレーションを必要とせず、以下のことが可能になります。

- インシデントの作成
- メールヘッダーの分析
- 送信者の IP アドレスの確認
- 送信ドメインの確認
- 送信者のレピュテーションのレビュー
- クレデンシャルフィッシングやマルウェアにつながるリンクの分析
- 添付を分析して脅威、マルウェア、またはその他のアクティブコンテンツを発見
- YARA ルールやマニュアル スクリプトの記述と維持を廃止

TRAP はメールから収集した情報のスコアリング、送信元の地域の特定、そして関連付けを行います。アナリストは潜在的脅威のサマリーを簡単に閲覧できます。

不正なメールのリスクを低減

メッセージングの管理者は「手動」または「自動 (Auto-pull)」で送信者のメールボックスから不正メールを取り除くことができます。TRAP は転送されたメッセージを追跡するために、転送のフォローとメーリングリストの展開をします (メーリングリストに転送されたメッセージも対象)。TRAP はメールを取り出して、隔離します。abuseメールボックスに送信された悪意のあるメールはすべてのユーザーの受信箱からも削除されため、全ユーザーのリスクを低減できます。

abuseメールボックスに大量のメールがあったとしても、CLEAR を使用すればフィッシングのリスクをすぐに減らすことができます。

メール報告のループを完成させる

エンドユーザーには、報告したメールの結果（実際に悪意のあるものであったのか、バルクメールだったのか、または問題なかったのか）がフィードバックされ、メール報告のループが完了します。これによって、組織の安全を守るためにメールを報告するという動機付けをすることができます。メールがバルクメールまたは問題ないものとしてスコア付けされた場合は、TRAPはそのインシデントを自動的にクローズします。そのためセキュリティチームはそれらを調査する必要はなくなり、負荷が軽減されます。悪意のあるメールではないメールのループはこれで完了します。

詳細

詳細は proofpoint.com/jp をご覧いただくか、 Proofpoint の営業担当にお問合せください。

注：上記の自動化には、*PhishAlarm*、*PhishAlarm Analyzer*、および *TRAP* のすべてが必要です。

PROOFPOINTについて
Proofpoint, Inc. (NASDAQ:PFPT) はサイバーセキュリティのトップ企業であり、組織の最大資産と最大リスクである人を守ります。クラウドベースのソリューションの統合スイートによってProofpointは世界中の企業が標的型脅威を阻止し、データを守り、ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。また、Fortune 1000の過半数を超える企業を含む、あらゆる規模のトップ企業がメールやクラウド、ソーシャルメディア、Web関連の最重要なセキュリティとコンプライアンスのリスクを緩和するためにProofpointに頼っています。詳細はwww.proofpoint.com/jpをご覧ください。

©Proofpoint, Inc. Proofpointは、米国およびその他の国におけるProofpoint, Inc.の商標です。記載されているその他すべての商標は、それぞれの所有者に帰属します。